AMENDMENTS TO CLAIMS:

This listing of claims will replace all prior versions and listings of claims in this application:

Claims 1-31 cancelled.

32. (New) A secure endorsed transaction system, comprising:

an encoder that generates a unique code from input data comprising transaction data and a human identifier that uniquely identifies a human being;

a digital signature processor that generates a digital signature by encrypting the unique code using a first key of an asymetrical key pair that includes the first key and a corresponding second key;

a formatter that formats a secure endorsed transaction using the digital signature and the input data; and

a verifier that verifies integrity of the secure endorsed transaction by, as a function of the secure endorsed transaction, comparing a stored unique code derived by decrypting the digital signature using the second key with a computed unique code derived from the human identifier and the transaction data.

33. (New) The system of claim 32, further including smart card input/output device for reading and/or writing data representing secure endorsed transactions from and/or to smart cards.

34. (New) The system of claim 33, further comprising:

means for receiving signals from the smart card device indicating the insertion of a smart card.

35. (New) The system of claim 33, wherein the smart card input/output device includes:

means for acquiring card data from a smart card for inclusion in a secure endorsed transaction.

36. (New) The system of claim 33, wherein the smart card input/output device includes:

means for dispatching data representing a secure endorsed transaction to a smart card.

37. (New) The system of claim 32, further comprising:

a biometric input device for receiving signals representing the human identifier that uniquely identifies a human being.

38. (New) The system of claim 32, further comprising:

means for receiving at least one of the first key and the second key.

39. (New) The system of claim 38, wherein the second key is received from a source external to the system.

40. (New) A method for processing secure endorsed transactions, comprising:

generating by an encoder a unique code from input data comprising transaction data and a human identifier that uniquely identifies a human being;

generating a digital signature by encrypting the unique code using a first key of an asymetrical key pair that includes the first key and a corresponding second key;

formatting a secure endorsed transaction using the digital signature and the input data; and

verifying integrity of the secure endorsed transaction by, as a function of the secure endorsed transaction, comparing a stored unique code derived by decrypting the digital signature using the second key with a computed unique code derived from the human identifier and the transaction data.

41. (New) The system of claim 32, further including smart card input/output device for reading and/or writing data representing secure endorsed transactions from and/or to smart cards.

42. (New) The system of claim 33, further comprising:

receiving signals from the smart card device indicating the insertion of a smart card.

43. (New) The system of claim 33, wherein the smart card input/output device includes:

acquiring card data from a smart card for inclusion in a secure endorsed transaction.

44. (New) The system of claim 33, wherein the smart card input/output device includes:

dispatching data representing a secure endorsed transaction to a smart card.

45. (New) The system of claim 32, further comprising:

receiving signals from a biometric input device representing the human identifier that uniquely identifies a human being.

46. (New) The system of claim 32, further comprising:

receiving at least one of the first key and the second key.

47. (New) The system of claim 38, wherein the second key is received from a source external to the system.

48. (New) A system for processing secure endorsed transactions, comprising:

means for generating a unique code from input data comprising transaction data and a human identifier that uniquely identifies a human being;

means for generating a digital signature by encrypting the unique code using a first key of an asymetrical key pair that includes the first key and a corresponding second key;

means for formatting a secure endorsed transaction using the digital signature and the input data; and

means for verifying integrity of the secure endorsed transaction by, as a function of the secure endorsed transaction, comparing a stored unique code derived by decrypting the digital signature using the second key with a computed unique code derived from the human identifier and the transaction data.

49. (New) The system of claim 32, further including smart card input/output device for reading and/or writing data representing secure endorsed transactions from and/or to smart cards.

50. (New) The system of claim 33, further comprising:

means for receiving signals from the smart card device indicating the insertion of a smart card.

51. (New) The system of claim 33, wherein the smart card input/output device includes:

means for acquiring card data from a smart card for inclusion in a secure endorsed transaction.

52. (New) The system of claim 33, wherein the smart card input/output device includes:

means for dispatching data representing a secure endorsed transaction to a smart card.

53. (New) The system of claim 32, further comprising:

a biometric input device for receiving signals representing the human identifier that uniquely identifies a human being.

54. (New) The system of claim 32, further comprising:

means for receiving at least one of the first key and the second key.

55. (New) The system of claim 38, wherein the second key is received from a source external to the system.

56. (New) The system of claim 55, wherein the second key is used by the verifying means to derive the computed unique code.